數字密碼的一些新研究

楊重駿、楊照崑

1.導 言

在書〔1〕中我們介紹了Diffie-Hellman在1976年發表了一種破天荒的數字密碼。它和往常密碼不同之處是，拍發及接受兩方都不必怕拍出的數字密碼中途被人截接偵破，只要收方保有一組解碼的數字組，用來把拍出的數字轉換成原來未拍出前的數字即可，其中所用的原理是整數論中的所謂「中國人剩餘定理」，也是國人所稱的「韓信點兵術」，及若僅知一個大數N，其爲兩個大質數p_1,p_2 的乘積（即$N=p_1p_2$），但要把這兩個質因子p_1，p_2找出是很困難的事實（一般如果N爲一個百位數，照目前已知找質數的方法及最快速的計算機來計算，日夜不停地進行計算，也至少要花上九年的時間。）所以Diffie-Hellman兩氏的密碼算是目前最具保密性的了。但在該法中，拍碼及譯碼（解碼）時都用到了大數的高冪次計算，所以計算量很大，這是一個缺點（但也確保了保密性）。

在1979年兩位華裔的工程師S.C.Lu及L.N.Lee，介紹了一個較D-H兩氏方法簡便多的一種密碼〔2〕，它也是利用中國人剩餘定理及找大質因子困難的事實，但發碼時只涉及幾個乘法及對模數的加法，譯碼時只涉及解一組二元一次方程式。雖然Lu-Lee兩氏在他們文中聲稱具有高度的保密性，但在文〔2〕發表的同年就有人撰文在〔4〕及〔5〕中指出Lu-Lee兩氏密碼的破綻。

1985年兩位印度工程師提出了一篇對Lu-Lee兩氏方法的修正文章〔3〕，並且聲稱此法至少可以抵擋〔4〕及〔5〕兩文中的破法。我們在本文中將先介紹Lu-Lee兩氏的密碼法及其破綻之處然後介紹、討論〔3〕文中所作的改進。最後我們把最近在數學界有關質數的檢驗法的進展當作補充資料作報導，希望讀者能用他山之石以攻錯的精神，在此方面作急起直追的努力。

2.Lu-Lee 密碼方法及原理

除非特別聲明外，本文用來代表未知數及已知數的文字都是指的整數。我們將就拍碼（或編碼）法及解碼（或譯碼）法作解說。

拍碼法：

設m_1及m_2爲兩個要送出的數字碼（或信息），我們可不妨限定$0<m_1<M_1$及$0<m_2<M_2$，M_1及M_2爲有關數碼m_1及m_2的上界。

以下我們要指出如何定此上界（這與解碼有關）。我們可以公開一組與拍碼有關的數字組（c_1, c_2, r）。

現所要拍出的數碼爲 x，

$$x \equiv (c_1 m_1 + c_2 m_2) \bmod r \tag{1}$$

解碼法：

收方必需具有一組可以由 x 得出 m_1 及 m_2 的解碼數字組（$a_{11}, a_{12}, a_{21}, a_{22}, p_1, p_2$），此組爲保密的。

則當甲方拍出 x 時，乙方作如下的計算：

$$x_1 \equiv x \pmod{p_1},\ x_2 \equiv x \pmod{p_2} \tag{2}$$

得了 x_1 及 x_2 後，m_1 及 m_2 可由下面分式得出：

$$m_1 = \frac{x_1 a_{22} - x_2 a_{12}}{a_{11} a_{22} - a_{12} a_{21}} \tag{3}$$

$$m_2 = \frac{x_2 a_{11} - x_1 a_{21}}{a_{11} a_{22} - a_{12} a_{21}} \tag{4}$$

任何一解碼必需要滿足對於拍出不同的 x，一定得出不同的 m_1 及 m_2 否則就混淆不知原來的數碼了，如何有此種保證？這與參數 c_1, c_2，r，及 $a_{11}, a_{12}, a_{22}, a_{21}$，$M_1$ 及 M_2 的選擇條件有關，以下我們就討論如何選取這些參數。

選參數的條件：

1. c_1 及 r，c_2 及 r 皆爲互質，r 爲兩個大質數 p_1, p_2 之乘積，即

$$(c_1, r) = (c_2, r) = 1,\ r = p_1 p_2 \tag{5}$$

並且進一步要求

$$c_1 + c_2 \geqslant r \tag{6}$$

現要保密的解碼參數組（$a_{11}, a_{12}, a_{21}, a_{22}, p_1, p_2$）6個參數都是要保密的，但它們之間要滿足下列關係：

2. $a_{11} \equiv c_1 \pmod{p_1}$，$a_{12} \equiv c_2 \pmod{p_1}$
$a_{21} \equiv c_1 \pmod{p_2}$，$a_{22} \equiv c_2 \pmod{p_2}$ (6)

並且要求

$$a_{11} a_{22} - a_{12} a_{21} \neq 0 \tag{7}$$

這是很明顯的一個要求。

3. M_1 及 M_2 要求滿足

$$M_1 \leqslant \left[\frac{1}{2} min\left\{\frac{q}{a_{11}}, \frac{q}{a_{21}}\right\}\right] \tag{8}$$

$$M_2 \leqslant \left[\frac{1}{2} Min\left\{\frac{q}{a_{12}}, \frac{q}{a_{22}}\right\}\right] \tag{9}$$

其中 $q = min\{p_1, p_2\}$，$[y]$ 表 y 的整數部份。

現我們看解碼成立的過程：

對式(1)兩邊取模數 p_1，由同餘的原理可得：

$$x_1 \equiv x \pmod{p_1} \equiv (c_1 m_1 + c_2 m_2) \pmod{p_1} \tag{10}$$

或
$$\begin{aligned} x_1 &\equiv x \pmod{p_1} \\ &\equiv [c_1 \pmod{p_1} m_1 + c_2 \pmod{p_1} m_2] \\ &\quad \pmod{p_1} \\ &\equiv (a_{11} m_1 + a_{12} m_2) \pmod{p_1} \end{aligned} \tag{11}$$

由條件(8)及(9)可知 $a_{11} m_1 + a_{12} m_2 \leqslant p_1$ 因而

$$x_1 = a_{11} m_1 + a_{12} m_2 \tag{12}$$

同理可得

$$x_2 = a_{21} m_1 + a_{22} m_2 \tag{13}$$

解方程式(12)及(13)可得 m_1 及 m_2，如(3)式及(4)式，此解的存在及唯一性是因爲 $a_{11} a_{22} - a_{12} a_{21} \neq 0$，又注意 m_1 及 m_2 皆爲整數。

讀者不難發現這個方法的計算量很少。

參數的選取：

大參數 p_1 及 p_2 的選取可依據 Solovay 及 Strassen [6] 所提出的有效的或然率選法。一旦 p_1 及 p_2 選了，就可選 a_{11}，a_{12}，a_{21}，及 a_{22} 滿足 $a_{11} a_{22} - a_{12} a_{21} \neq 0$，然後由於 p_1 及 p_2 互質，由 Enclid的輾轉相除法可得：

$$b_1 p_1 + b_2 p_2 = 1 \tag{14}$$

對上式兩邊同乘以（$a_{21} - a_{11}$），經併項後可得

$$c_1 \equiv [(a_{21}-a_{22})b_1p_1+a_{11}] (mod r) \quad (15)$$

或

$$c_1 \equiv [(a_{11}-a_{21})b_2p_2+a_{21}] (mod r) \quad (16)$$

上式中 $r = p_1p_2$ 。同理可得

$$c_2 \equiv [(a_{22}-a_{12})b_1p_1+a_{12}] (mod r) \quad (17)$$

或

$$c_2 \equiv [(a_{12}-a_{22})b_2p_2+a_{22}] (mod r) \quad (18)$$

下面我們舉一個實際計算的例子（〔2〕文中的）。由此例子我們可得到一點端倪，爲何此法易被偵破了。（當然參數選取的種種限制也多少提供了一些線索）。

例子：取 $p_1=97$，$p_2=103$，及 $a_{11}=3$，$a_{12}=2$，$a_{21}=5$，$a_{22}=4$ 作爲解碼的參數組（這是要保密的）現 $r=p_1p_2=9991$ 及 $1=17\times97-16\times10^3$ 可得 $b_1=17$，$b_2=-16$ 於是發碼的參數組（c_1，c_2，r）（這是要公開的）中的 c_1 及 c_2 可得如下：

$$c_1=2\times17\times97+3=3301$$

$$c_2=2\times17\times97+2=3300$$

現我們能拍送的數字碼 m_1 及 m_2 能有多大？

$$M_1 \leqslant [\frac{1}{2}min(\frac{97}{3}, \frac{97}{5})]=9$$

$$M_2 \leqslant [\frac{1}{2}min(\frac{97}{2}, \frac{97}{4})]=12$$

換句話 m_1 及 m_2 的選擇不能分別大於9及12，現我們比方取 $m_1=7$，$m_2=5$（或用二進位制 $m_1=0111$ 及 $m_2=0101$）。

拍發的明碼爲

$$x \equiv [7\times3300+5\times3300] (mod 9991)$$

$$\equiv 9634$$

因而

$$x_1=9634 (mod 97)=31$$

$$x_2=9634 (mod 103)=55$$

解

$$3m_1+2m_2=31$$

$$5m_1+4m_2=55$$

得到 $m_1=7$ 及 $m_2=5$，即原來的數字信息。

在文〔2〕中Lu-Lee 兩氏也曾討論了一些可能的破碇，不過他們總結只要 p_1 及 p_2 取的夠大，及一般 a_{ij} 也取的相當大就可避免被偵破的危險，但 a_{ij} 一大，M_1 及 M_2 就要減小了，這個矛盾是在〔3〕文中所要對付的，下面我們就介紹此一改進的方法。

首先在〔3〕文中指出的是在〔4〕及〔5〕的兩篇文中利用拍送出不同的明碼，經過譯碼得到不同的原碼的事實，Lu-Lee 兩氏的密碼可以不必知道 p_1 及 p_2，照樣可把 m_1 及 m_2 求出。另外在文[5]中指出由於當 c_i（$i=1,2$）取 p_1 或 p_2 爲模所得的剩數 a_{ij} 值都很少（這是因爲要求 $a_{i1}m_1+a_{i2}m_2<p_i$，$i=1,2$）所以依此事實可以把 p_1 及 p_2 求出，之後可求得 a_{ij}。

3. Lu-Lee 法的改進

參數選取：

如同在Lu-Lee法一樣，譯碼的秘密解碼組爲一組數（p_1，p_2，a_{ij}，$i=1,2$，$j=1,2$）及公開的發碼，參數組爲（c_1，c_2，r）但要求 a_{ij} 滿足

(i) a_{ij} 爲 4 個連續數（這個條件是本文作者附加的，這個加添似乎是對解碼時需要的）。

(ii) $a_{12} > a_{22}$

(iii) $a_{21} > a_{11}$

(iv) a_{ij}，$i=1,2$，$j=1,2$ 每個值不小於 2^{200}（或二進位制 200位的數字）。

(v) 對於 M_1 及 M_2 我們要求 $M_1 \leqslant 2^{50}$，$M_2 \leqslant 2^{50}$。

假定我們固定取 p_1 及 p_2 皆爲二進位下具有252位數的值，（因而 r 爲一在二進位表示具有 504位數的值）就可以使得 (v) 滿足了。

發碼：

(a)首先我們要求發的數碼 m 不大於 2^{199}（即在二進位下至多爲一個 199位數）。

(b)任選一組整數（m_1，m_2），$m_1 \leqslant M_1$，$m_2 \leqslant M_2$

,拍出下列明的數字碼

$$m_e \equiv (m + c_1 m_1 + c_2 m_2)(mod r)。$$

換句話，把Lu-Lee中的明碼加上了一個因子$m(modr)$，注意的是這時我們是一次送一數碼，解一數碼。

我們首先看這個密碼法，會不會產生混淆，即不同的原碼m及m'其相應的m_e及m_e'是否可能會相同？

所以我們假設$m \neq m'$看$m_e = m_e'$可不可能？今

$$\begin{aligned} m_e &\equiv (c_1 m_1 + c_2 m_2 + m)(modr) \\ &\equiv \{(c_1 m_1 + c_2 m_2)(modr) \\ &\quad + m(modr)\}(modr) \\ &\equiv (x_e + m)(modr) \end{aligned}$$

同理可得

$$m_e' \equiv (x_e' + m)(modr)$$

及

$$\begin{aligned} m_e(modp_1) &\equiv \{x_e(modp_1) + m(modp_2)\} \\ &\quad (modp_1) \\ &\equiv (x_1 + m)(modp_1) \qquad (19) \end{aligned}$$

$$m_e(modp_2) \equiv (x_2 + m)(modp_2) \qquad (20)$$

$$m_e'(modp_i) \equiv (x_i' + m')(modp_i) \; ; i = 1, 2 \qquad (21)$$

於是由$m_e = m_e'$兩邊取p_i爲模數的餘式相等下，利用上面三式可得：

$$(x_i + m)(modp_i) \equiv (x_i' + m')(modp_i) \; ; i = 1, 2 \qquad (22)$$

即

$$(x_i - x_i')(modp_i) \equiv (m - m')(modp_i) \; ; i = 1, 2$$

因m, m', x_i, x_i'皆小於p_{ij}，$i = 1, 2$。故

$x_i - x_i' = (m - m')$；$i = 1, 2$因而

$$x_1 - x_1' = m - m' = x_2 - x_2' \qquad (23)$$

注意$|(m - m')| \leqslant a_{ij}$；$i = 1, 2$及$j = 1, 2$依定義

$$\begin{cases} x_1 = a_{11} m_1 + a_{12} m_2 \\ x_2 = a_{21} m_1 + a_{22} m_2 \end{cases}$$

及

$$\begin{cases} x_1' = a_{11} m_1' + a_{12} m_2' \\ x_2' = a_{21} m_1' + a_{22} m_2' \end{cases}$$

由上面兩組方程組及(23)可得

$$\begin{aligned} &a_{11}(m_1 - m_1') + a_{12}(m_2 - m_2') = a_{21}(m_1 \\ &- m_1') + a_{22}(m_2 - m_2') \qquad (24) \end{aligned}$$

於是

$$(a_{11} - a_{12})(m_1 - m_1') = (a_{22} - a_{12})(m_2 - m_2') \qquad (24)$$

由於上式兩方必須爲同號，故$m_1 - m_1'$或$m_2 - m_2'$同爲正或同爲負。若同爲正，則依據式(23)，由式(24)可得：

$$\begin{aligned} m - m' = x_1 - x_1' &= a_{11}(m_1 - m_1') + a_{12}(m_2 - \\ &m_2') > a_{11} + a_{12} \end{aligned}$$

此與m與m'之大小規定不符，同樣在$m_1 - m_1'$及$m_2 - m_2'$同爲負時亦可得同樣的矛盾，所以若$m \neq m'$，則$m_e \neq m_e'$。

4.改進碼的解碼步驟

計算 $m_{ei} \equiv m_i(modp_i)$；$i = 1, 2$ (25)

解下列連立方程組（未知數爲t_1及t_2，其解可能爲有理數，不一定爲整數）。

$$\begin{cases} a_{11} t_1 + a_{12} t_2 = m_{e1} \\ a_{21} t_1 + a_{22} t_2 = m_{e2} \end{cases} \qquad (26)$$

取 $k_1 = [t_1]$及$k_2 = [t_2]$ (27)

計算 $a_{i1} k_1 + a_{i2} k_2 = m_{ei}'$；$i = 1, 2$ (28)

取 $m = m_{ei} - m_{ei}'$ (29)

我們現看上面每一步驟是否合理？主要是找出步驟(26)中m_{e1}與m_{e2}及檢驗步驟(29)。

任何一有理數t都可成式$t = [t] + (t - [t])$＝整數部份＋小數部份。所以不妨設

$$t_i = [t_i] + r_i / \Delta$$

$$\Delta = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11} a_{22} - a_{21} a_{12}$$，r_i爲一適當

的有理數，使得 r_i/Δ 爲 t_i 之小數部分。

現我們把步驟㉖中的方程組改寫爲下面的形式：

$$\begin{cases} a_{11}t_1+a_{12}t_2=x_1+m \\ \quad (\text{即以 } x_1+m \text{表} m_{e1}, x_1 \text{爲一參數}) \\ a_{22}t_1+a_{22}t_2=x_2+m \\ \quad (\text{即以 } x_2+m \text{表} m_{e2}, x_2 \text{爲一參數}) \end{cases}$$

以下我們將證明 x_i 爲步驟㉘中的 m_{ei}'；$i=1,2$。這樣步驟㉙亦成立，原數碼也就得到了。

解上面方程組得

$$\begin{cases} t_1=(a_{22}x_1-a_{12}x_2)/\Delta+m(a_{22}-a_{12})/\Delta \\ t_2=(a_{21}x_1-a_{11}x_2)/-\Delta+m(a_{21}-a_{11})/-\Delta \end{cases}$$

由於我們將希望看到的是 x_i 爲 m_{ei}'（$=a_{i1}k_1+a_{i2}k_2$），所以我們不妨設

$$\begin{cases} x_1=a_{11}m_1+a_{12}m_2 \\ x_2=a_{21}m_1+a_{22}m_2 \end{cases}$$

再證明 m_1 與 m_2 事實上分別等於 k_1 及 k_2 就得了。

由上面方程組可得：

$$\begin{cases} m_1\Delta=a_{22}x_1-a_{12}x_2 \\ m_2\Delta=-a_{21}x_1+a_{11}x_2 \end{cases}$$

將此組結果代入 t_1 及 t_2 之值中得

$$\begin{cases} t_1=m_1+m(a_{22}-a_{12})/\Delta \\ t_2=m_2+m(a_{21}-a_{11})/-\Delta \end{cases}$$

由於參數選取的條件，可驗證得 $m(a_{22}-a_{12})/\Delta$ 及 $m(a_{21}-a_{11})/-\Delta$ 皆爲小數。（利用：$-\Delta=-a_{11}a_{22}+a_{12}a_{21}\geqslant(a_{11}+1)(a_{22}+1)-a_{11}a_{22}\geqslant a_{11}+a_{22}$，及參數選取條件(i)，可得 $|a_{22}-a_{12}|\leqslant 3$，$|a_{21}-a_{11}|\leqslant 3$）。故我們得下面結果

$$[t_1]=m_1 \text{ 及 } [t_2]=m_2$$

因而在解碼的步驟㉘中所計算的爲方程組

$$\begin{cases} x_1=a_{11}m_1+a_{12}m_2 \\ x_2=a_{21}m_1+a_{22}m_2 \end{cases}$$

中的 x_1 及 x_2

有了 $\begin{cases} x_1=m_{e1}' \text{ 及 } x_2=m_{e2}' \end{cases}$

因而 $\begin{cases} x_1+m=m_{e1} \text{ 及 } x_2+m=m_{e2} \end{cases}$

步驟㉙也就自然成立了。

5.補充資料

爲了提起讀者研究的興趣，我們在此順便介紹最近在美國科學雜誌（Science, vol.231 1985, p.452-453）報導的有關質數檢驗法的一些最新發展。

過去十年以來，出現了許多有關質數的檢驗，但都有它們獨特的短處，所以迄今爲止仍無一個十全十美的方法。在1975年左右任職哈佛大學及希伯來大學的M. Rabin 分別與 伯克萊加州大學的R. Solovay 及瑞士蘇黎士（Zurich）大學的V. Strassen兩人小組，各自發現了一種或然率的質數檢驗法，此檢驗法容易且快速。所謂快速是指用計算機來照此方法的程序運算，所需的時間是多項式時間（Polynomial time 較具體的講，所需的四則運算的次數爲 $\leqslant cn^k$，n 爲所要測的正整數，k 及 c 爲兩常數。）但由於它的或然性，使得一般人存疑，也因此不敢照用此法。這個方法使得當一個人用它去試一個數，如果檢驗得出的答案是非質數，他一定可以相信（也即結論一定是正確的），但如果得出是質數的答案，那就不一定百分之百的可信了。因此理論上這個方法不能用來檢驗那個數爲質數。

幾乎在同時，南加大的G. Miller 發現了一個非或然性的質數檢驗法。他的方法可以很快(多項式時間)地把一個原非質數的數，正確地判斷出來。但若一個數經檢驗得的結論是質數的話，是不是一定正確，却要看數學上有名的推廣的黎曼氏假說（Extended Riemann Hypothesis）是否成立而定。因此假如該假說被證明是錯誤的話，許多由Miller氏判定的

質數，事實就是非質數了。

所以自然就有人試著把這些或然的性質，或上面方法中與假說相連的缺陷從方法中除去。果然在1980年三個美國數學家L.Adleman（南加大），R.Rumley及C.Pomernance（伊里諾大學）得到了一個相當快而且具果斷性的檢驗法。他們的方法可以正確地判斷一個數爲質數或非質數，但其缺陷是計算速度不夠快（超過多項式時間），仍無法改進到多項式的時間。

最新的一個方法是由麻省理工學院的兩位數學家Goldwasser及Kilian的或然性檢驗法。（這裡的或然性與前面提的或然性兩者意義上不同），這個方法很快（只需多項式時間）就可以把一個非質數的數正確的判定出來，對於質數也可以作正確的判斷，但其理論上就是可能對一小部份（比例上而言）的質數，這個方法判斷的時間不很快（即超過多項式時間），也就是因爲有這樣一個可能很小的機會，運算時間較長，所以仍把這個方法歸之於或然性的檢驗法，但有趣的是迄今爲止還未有人找出一個需要超過多項式時間來判斷的質數例子！而且如果眞的找出如此一個質數，將會轟動數學界，因爲這與數論上一個有關質數分佈密度的有名的猜測有關。

在K-G兩氏的方法及其它一些類似的方法中，主要與研究所謂的橢圓曲線上的整數點及其階（rank）的高深研究有關，而這方面的研究，原來是與解決討論下列的一個問題有關:

設$p(x,y)$爲x,y的一個齊次多項式（如$p(x,y)=x^2-3y^2$），m爲任一整數，以$N_P(m)$表滿足方程式

$$p(x,y)=m$$

的所有整數解的個數。

我們已知的是$N_P(m)$總爲有限的（其值當與p及m有關），但如何求出那些整數解及精確判斷$N_P(m)$的界限，這些一直都是數論中漂亮而且艱深的研究課題。

參考文獻

1.楊重駿、楊照崑，整數論及其應用。東華書局。

2.S.C.Lu & L.N.Lee, A simple and effective public-key cryptosystem, COMSAT TECHINICAL RENEW vol.9, No.1, 1979, pp.15-24。

3.B.S.Adiga & P.Shankar, Modified Lu-Lee Cryptosystem, *Electronics Lelters*.

4.L.M.Adleman & R.L.Rivest, How to break the Lu-Lee (COMSAT) public-key cryptosystem, *MIT Laboratory for Computer Science*, July 1979.

5.M.J.Kochonski, Remarks on Lu & Lee's proposal, *Cryptologia*, 1980.

6.R.Solovay & V.Strassen, A fast Monte-Carlo Test for primality, SIAM Jour. *on Computer*, March 1977, pp.84-85.

～本文作者分別任職於美國海軍研究實驗所及佛羅里達大學統計系～